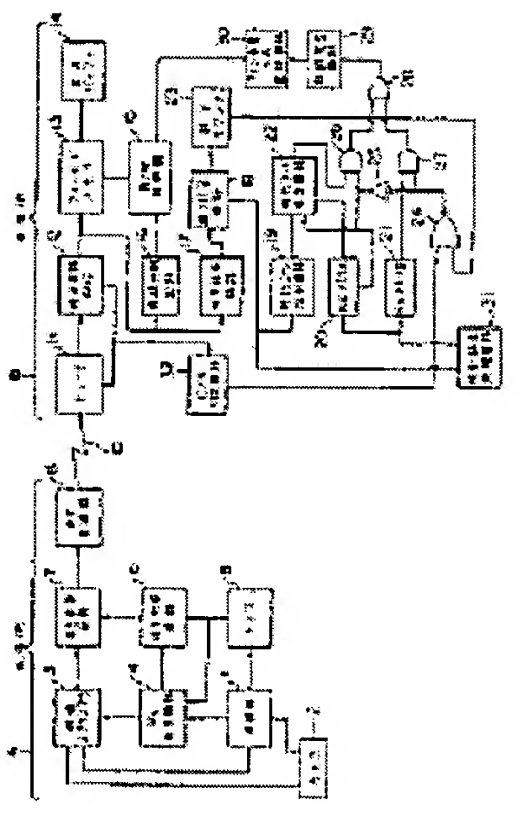
TRANSMISSION SYSTEM FOR DECODING KEY

Patent number: JP2041046
Publication date: 1990-02-09
Inventor: HIRASHIMA MASAYOSHI
Applicant: CONDITIONAL ACCESS TECH
Classification:
- international: ***H04H1/00; H04L9/06; H04L9/14; H04L9/34; H04N7/167;*** **H04H1/00; H04L9/06; H04L9/14; H04L9/34; H04N7/167;** (IPC1-7): H04H1/00; H04L9/06; H04L9/14; H04L9/34; H04N7/167
- european:
Application number: JP19880190599 19880801
Priority number(s): JP19880190599 19880801

Abstract of **JP2041046**

PURPOSE:To attain release of scrambling even if C/N(carrier/nose) is deteriorated by sending a decoding key at a comparatively short time interval and sending plural release keys each intermittently or continuously in relation with time information.

CONSTITUTION:When the C/N reaches a certain value or below, an output of a C/N discrimination circuit 32 goes to a high level. Then an output of an OR gate 24 goes to a low level, an AND gate 27 is cut off and an output of an inverter 25 goes to a high level and an AND gate 26 is conductive. A time code collation circuit 22 starts the collation after an output of the inverter 25 goes to a high level. Then a data Ks20 of a Ks memory A 20 is read and given to a random number generating circuit 29 via the AND gate 26 an OR gate 28 and a conversion circuit 30 converts a generated random number into a line number. Thus, while the decoding key Ks is being switched continuously, descrambling is continued.



⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2-41046

⑤1Int.Cl.⁵		識別記号	庁内整理番号			
H 04 H	1/00	F	7608-5K			
H 04 L	9/06					
	9/14					
	9/34					
H 04 N	7/167		8725-5C			
			7240-5K	H 04 L	9/00	B
			7240-5K		9/02	Z

⑬公開　平成2年(1990)2月9日

審査請求　有　請求項の数 3　(全7頁)

⑤4発明の名称　解読鍵の伝送方式

⑳特　願　昭63-190599
㉒出　願　昭63(1988)8月1日

⑦2発明者　平嶋　正芳　東京都港区虎ノ門1丁目20番7号　株式会社コンデイショナル・アクセス・テクノロジー研究所内

⑦1出願人　株式会社コンデイショナル・アクセス・テクノロジー研究所　東京都港区虎ノ門1丁目20番7号

⑦4代理人　弁理士　浅村　皓　外3名

明　細　書

1. 発明の名称

解読鍵の伝送方式

2. 特許請求の範囲

(1)　送信側から受信側へ情報を伝送するに際し、送信側で前記情報を分割しかつ分割された情報の順序を並べ替えると共に、受信側で解読鍵を用いて元の順序に並べ直し前記情報を再現する伝送方式において、前記解読鍵を比較的に短い時間間隔で変化させ、前記時間間隔で1個ずつ伝送すると共に、併せて前記解除鍵を複数個ずつ時刻情報と関連させて間欠的又は連続的に伝送することを特徴とする解読鍵の伝送方式。

(2)　請求項(1)において、複数個の前記解読鍵のそれぞれに時刻情報を対応させ、前記時刻情報と前記解読鍵とを一緒に伝送することを特徴とする解読鍵の伝送方式。

(3)　請求項(1)又は(2)において、受信側で信号伝送路のC／Nの変化を検出し、前記C／Nの変化に対応して、使用すべき鍵を、個別に伝送される鍵と時刻情報に対応させてまとめて伝送される鍵とのいずれかに切り替えることを特徴とする解読鍵の伝送方式。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明は放送システムにおけるスクランブルを解除するための解読鍵の伝送方式に関する。

〔従来の技術〕

衛星放送等の有料放送システムでは視聴契約の加入者のみに番組が提供されるように、放送局において番組信号にスクランブルをかけて送信を行う。一方、加入者の側ではスクランブル鍵を用いてスクランブルを解除し番組信号を取り出す。これにより加入者のみの番組視聴を可能にし、不正視聴を防止する。スクランブルされた番組信号をデスクランブルするためのスクランブル鍵は一般に番組信号と同じ伝送路で例えば毎秒ごとに伝送されるが、このような場合、スクランブル鍵の不正解読を防ぎ不正視聴を確実に防止するために、毎秒送られるスクランブル鍵を短時間（例えば

１０秒）で変更する。

〔発明が解決しようとする問題点〕

スクランブル鍵を短時間で変更して送る方式では、受信側でスクランブル鍵が送られてくる度に取り出してスクランブルを解除しなければならない。このような場合、例えば、ＦＭを利用する衛星放送において、降雨又はアンテナの向きが狂う等の理由によりＣ／Ｎ（carrier とnoise との比）が低下すると、映像、音声、制御信号にノイズが多数入り、スクランブル鍵を正確に取り出すことができなくなる。この結果受信側においてスクランブルの解除が不可能になる。特に、スクランブル鍵を１０秒に１回変更するシステムにおいては、スクランブル鍵の受信を１回誤まると１０秒の間スクランブルを解除することができないという不具合が生じる。

〔問題点を解決するための手段〕

本発明に係る解読鍵の伝送方式は、送信側で番組等の情報を分割し、分割したものの順序を並べ替えて受信側へ伝送し、受信側で情報と同一伝送路で伝送されてくる解読鍵を用いて元の順序に並べ直し情報を再現する伝送方式において、前記解読鍵を比較的に短い時間間隔で変化させかつこの時間間隔で伝送すると共に、併せて解除鍵を時刻情報と関連させて複数個ずつ間欠的又は連続的に伝送するようにしている。

〔作用〕

受信側では伝送路のＣ／Ｎの状態を検出し、Ｃ／Ｎの状態に対応してスクランブル解除するために使用する鍵を決定する。解読鍵を時刻情報に対応させて複数個まとめて伝送するようにしたから、所定時間内で一度でも正しく解読鍵を受信できれば、Ｃ／Ｎが低下した場合でも先に受信した鍵を使用することによつてスクランブル解除を行うことが可能となる。

〔実施例〕

以下に本発明の好適実施例を添付図面に従つて説明する。

第１図は本発明に係る放送システムをブロツク図で示したもので、第１図中左側のＡは送信側の回路構成であり、右側のＢは多数の受信側の１つを示す回路構成である。この実施例では一例として送信側Ａと受信側Ｂとを結ぶ伝送路１０として衛星放送電波を利用している。従つてこの放送システムは衛星を利用した有料放送システムであり、不正視聴を防止する目的で映像信号と音声信号の両方にスクランブルがかけられている。以下の説明では説明の便宜上映像のスクランブルについてのみ説明する。また伝送路１０におけるＣ／Ｎ（carrierとnoise との比）の劣化は１回につき３０秒以内と仮定する。

第１図に示された回路の構成を説明する。

送信側Ａにおいて、１は送信側の同期盤、２は信号源としてのカメラ（ＶＴＲやディスクでもよい）、３はカメラ２の映像出力にスクランブルをかけるスクランブラー、４はスクランブルをかけるための乱数の基準となる鍵Ｋｓを発生させるＫｓ発生回路であり、同期盤１で同期をとつている。鍵Ｋｓはスクランブルを解除するための解読鍵である。５は同期盤１に同期しているタイマ、６は第２図のＡ，Ｂに示す信号形式で鍵Ｋｓやその他の情報を送出するための信号形成回路、７は第２図Ａ又はＢの形式の信号をテレビ信号中のＶＢＩ（垂直帰線期間）の１水平走査期間に重畳する重畳回路である。タイマ５はＫｓ発生回路４と信号形成回路６との同期をとつている。８はＲＦ変調器であり、このＲＦ変調器８の出力が衛星を介し、日本全国に散在する多数の受信局の各受信アンテナ（図示せず）へ伝送される。

受信側Ｂにおいて、受信アンテナから図示しないＬＮＢ（Low Noise Block down convertor）を経てチユーナ１１へＲＦ変調器８の出力が供給される。チユーナ１１では、受信した信号を選択し、中間周波（例えば約４００MHz）に変換し、検波回路１２でＦＭ検波する。また検波回路１２はＡＧＣ電圧も発生し、これをチユーナ１１へ帰還している。チユーナ１１と検波回路１２は通常のＢＳチユーナの回路と同一である。１３は検波回路１２の出力信号を２フィールド分ストアするフィールドメモリであり、２つの１フィールドメモ

リから成る。１４は出力バツフア、１５はフィールドメモリ１３の書込みと読出しを制御するＲ／Ｗ制御器である。１６は検波回路１２から出力されるテレビ信号から同期信号を分離する同期分離回路、１７は上記テレビ信号からＶＢＩ中の各種信号を取り出すための信号抜取回路であり、この回路は送信側Ａから送られてくる第２図Ａ，Ｂに示される信号を抜き取り、サンプリングしてディジタル信号に変換する。１８は文字放送で使用されているものと同一ないわゆるＢＥＳＴ方式と呼ばれる誤り訂正回路である。誤り訂正回路１８の出力信号は、誤りカウンタ２３、時刻コード抜取回路１９、暗号・課金処理回路３１に供給される。暗号・課金処理回路３１で得られた情報はＫｓメモリＡ２０とＫｓメモリＢ２１に供給され、これらのメモリのそれぞれに記憶される。２２は時刻コード照合回路であり、この回路には時刻コード抜取回路１９とＫｓメモリＡ２０の各出力が入力される。また３２はＣ／Ｎ判定回路で、検波回路１２から出力されるＡＧＣ電圧によつてＣ／Ｎの状態を判定する。受信側Ｂはその他に、ＮＯＲゲート２４、インバータ２５、ＡＮＤゲート２６，２７、ＯＲゲート２８を含む。ＮＯＲゲート２４はＣ／Ｎ判定回路３２と誤りカウンタ２３の各出力を入力し、その出力をインバータ２５とＡＮＤゲート２７へ与える。インバータ２５はその出力をＫｓメモリＡ２０と時刻コード照合回路２２とＡＮＤゲート２６に与える。ＡＮＤゲート２６の残りの入力には時刻コード照合回路２２の出力が入力され、またＡＮＤゲート２７の残りの入力にはＫｓメモリＢ２１の出力が入力される。ＡＮＤゲート２６，２７の各出力はＯＲゲート２８に与えられる。２９は乱数発生回路、３０はライン番号への変換回路であり、ＯＲゲート２８の出力を受けて乱数発生回路２９が乱数を発生し、ライン番号への変換回路３０を経て前述のＲ／Ｗ制御器１５に対して制御用信号を与える。

次に第１図に示された回路の作用について説明する。

送信側Ａでの映像信号にスクランブルをかける動作は映像スクランブラ３において行われる。映像スクランブラ３において、カメラ２から出力された映像信号はＫｓ発生回路４から与えられる鍵Ｋｓによつてスクランブルをかけられる。スクランブルをかけるために使用された鍵Ｋｓ及びその他の信号は、信号形成回路６を経て信号重畳回路７に与えられ、この信号重畳回路７で、映像スクランブラ３から供給されるスクランブルをかけられた映像信号のＶＢＩの１水平走査期間の中に重畳され、その後ＲＦ変調器８を経て受信側へ送出される。

次に受信側Ｂにおけるデスクランブル動作を簡単に述べる。ＫｓメモリＢ２１において得られる２４ビツトの鍵Ｋｓを用いて乱数発生回路２９でＰＮ系列（$2^{24}-1$）を発生させ、このＰＮ値を用いて変換回路２９で予め決めた手順（例えば、８ビツトの数をＲＯＭで変換する）に従つてライン番号（水平走査線の番号）に変換し、この番号を用いて、フィールドメモリ１３の中から正しい順序で信号を読み出し、出力バツフア１４を介してＣＲＴ等のディスプレイに元の画面を表示する。かかる動作は、テレビ画面を送信側でスクランブルし、その後受信側でデスクランブルする一例であり、特にラインパーミユテーションと呼ばれている。この場合、送信側Ａの映像スクランブラ３で使用される乱数、それに基づくライン番号、及びその順序は、受信側の乱数発生回路２９と変換回路３０で行われる作用と互いに逆（相補関係）になつている。

前記回路の作用を更に詳しく説明する。スクランブルシステムでは鍵Ｋｓ以外にも各種情報を送受する必要がある。現在放送されている日本の衛星放送の場合、ＰＣＭ音声の他にデータも送れる。この実施例では、一般的に適用できる方式としてＶＢＩの１Ｈを用いる例を考える。毎フィールド１Ｈを使い、１Ｈ中ヘツダーを除く１８４ビツトを制御情報その他に使うものとする。鍵Ｋｓを１０秒毎に変更すれば、鍵Ｋｓは１０秒に１回送出すればよい。この間のフィールド数は６０×１０＝６００フィールドであり、残りの５９９Ｈを利

用して鍵Ｋｓ以外の情報を送ることができる。また毎秒１０回余分にＫｓを送るものとすれば１０秒間に１０×１０Ｈ、すなわち１００Ｈを使うことになる。従つて、この場合には６００Ｈ中１０１Ｈを鍵Ｋｓの伝送に使う。以下においてはこの条件に基づいて説明する。残りの６００－１０１＝４９９Ｈの各１Ｈ当り１４４ビツトを各種制御や端末アクセス等についての制御情報に割当てることができる。

第２図はＶＢＩの１Ｈに含まれる２種類のデータパケツトを示す。Ａは鍵Ｋｓの情報を送るデータパケツトであり、Ｂは鍵Ｋｓ以外の制御情報を送るデータパケツトである。データパケツトＡでは鍵Ｋｓは２４ビツトであり、鍵Ｋｓを例えば6個（ｎ＝６）まとめて送るようにしている。またデータパケツトＡ，Ｂにはそれぞれ６ビツトのヘツダーと４０ビツトの時刻コード等の情報が含まれている。ヘツダーの内容については第３図に示される。

検波回路１２で出力されるスクランブルされた映像信号はフィールド毎にフィールドメモリ１３内の第１及び第２の１フィールドメモリにフィールドの順序に従つて交替させて記憶される。Ｒ／Ｗ制御器１５がフィールドメモリ１３における書込みと読出しを制御することにより受信側のデスクランブルが行われる。すなわち、Ｒ／Ｗ制御器１５は、第ｎフィールドのスクランブルされた映像信号を検波回路１２からそのままフィールドメモリ１３の中の第１の１フィールドメモリに書き込み、この間、第２の１フィールドメモリに書き込まれている第ｎ－１フィールドの映像信号を、変換回路３０の指示に従い、ＣＲＴ等の表示装置上で正常な映像が見えるような順序で走査線単位に読み出す。また、第ｎ＋１フィールドの映像信号では、第２の１フィールドメモリへ検波回路１２の出力する映像信号をそのまま書き込み、この間第１のフィールドメモリから第ｎフィールドの映像信号を、変換回路３０の指示に従い、ＣＲＴ等の表示装置上で正常な画が見えるような順序で走査線単位に読み出す。これをフィールド毎に繰返すことによりデスクランブル動作が継続される。

誤り訂正回路１８における誤り訂正は、第２図Ａ，Ｂの１９０ビツトの部分に対して行われる。この１９０ビツト中の、１４４ビツトは暗号化されている。暗号化部分は暗号・課金処理回路３１の暗号処理部で復号され、時刻コードと一緒にＫｓメモリＡ２０又はＫｓメモリＢ２１に記憶される。ＫｓメモリＢ２１には現在フィールドメモリ１３から読み出すための鍵Ｋｓが記憶され、ＫｓメモリＡ２０には将来のフィールドメモリ１３からの読み出しに使う鍵Ｋｓが複数個時刻コードと共に記憶されている。

ここでＣ／Ｎが低下して誤りが増加した場合を考える。Ｃ／Ｎが低下すると、検波回路１２のＡＧＣ電圧が上昇（又は下降）する。Ｃ／Ｎがある値以下になると、Ｃ／Ｎ判定回路３２の出力が高レベルになる。Ｃ／Ｎ判定回路３２の出力が高レベルとなると、ＯＲゲート２４の出力が低レベルとなり、ＡＮＤゲート２７は遮断され、またインバータ２５の出力が高レベルとなつてＡＮＤゲート２６が導通する。また誤り訂正回路１８での誤り訂正の回数が一定値以上になると、誤りカウンタ２３から高レベルが出力され、ＯＲゲート２４の出力が低レベルとなり、ＡＮＤゲート２６が導通し、ＡＮＤゲート２７が遮断される。時刻コード抜取回路１９では、第２図Ｂの形式の制御信号以外の非暗号化部の時刻コード××分△△秒（ＢＣＤで４×４＝１６ビツト）を受信する。この時刻コードが例えば６フィールド毎に送られているものとすると、約０．１秒毎に時刻コードが変化する。一方、ＫｓメモリＡ２０には××分△△秒という時刻コードと共に、第２図Ａの鍵Ｋｓが６個入つている。仮に△△秒として１０秒であるとすると、１０～１９秒の時刻コードが送られている間は、第４図に示すＫｓ10～Ｋｓ20が、第２図Ａの形式で送られており、Ｃ／Ｎが低下しないとき及び誤り訂正の個数が少ないときには、ＫｓメモリＡ２０へは第２図Ａの信号を受信する毎にＫｓ10～Ｋｓ00の２４×６ビツトを書き込ん

でいる。××分15秒でC／Nが低下し、インバータ25の出力が高レベルになつたとすると、それ以降KsメモリA20の書換えは中止される。その時の内容は第4図の通りである。××分15秒の時刻までは正常受信であつたから、KsメモリB21の記憶内容は第4図のKs10と同じである。時刻コード照合回路22はインバータ25の出力が高レベルになつた後照合を始める。しかし、C／Nが低下していると、第2図A，Bに示される時刻コードに誤りが含まれていることが多いので、時刻コード照合回路22は内部にタイマを有し、インバータ25の出力が低レベルの間（C／Nが高い時）、時刻コード抜取回路19の出力でタイマを較正する。C／N低下が1日中続くことはない。ここではC／N低下の期間を30秒以下と考えているので、その間タイマが進み遅れすることはない。従つて、時刻コードは時刻コード照合回路22の中で分秒4桁を形成し、そのコードと第4図の分秒のコードとを比較する。従つて、××分20秒になると、KsメモリA20の中の××分20秒のデータKs20を読み出し、これをANDゲート26及びORゲート28を経て乱数発生回路29へ伝え、乱数発生回路29でKs20を基にして乱数を発生させ、この乱数から変換回路30でライン番号へ変換する。以上の動作は、C／Nが高い時と同じである。例えば××分44秒にC／Nが高くなつて、C／N判定回路32の出力と誤り訂正カウンタ23の出力の両方が低レベルになると、KsメモリB21の出力（Ks50）がANDゲート27及びORゲート28を介して乱数発生回路29へ××分50秒に伝えられる。××分44秒から××分50秒まではKsメモリA20から読み出されたKs40に基づいて発生した乱数が使われる。××分50秒には、第5図に示されるKs50～Ks40′が送られ、KsメモリA20へ書き込まれる。この場合、KsメモリB21へ書き込まれるKs50を、第2図Bで先に送り，次のフィールドでは第2図Aで送る。必要なら、第2図Bを、××分50秒の寸前（2フィールド以上前）に続いて第2図Aを送るようにしてもよい。このようにすれば、連続して鍵Ksを切り換えつつデスクランブルし続けることができる。なお、鍵Ksを切換時刻よりも先に送る時は、時刻コード照合回路22で、KsメモリB21の内容についても時刻コードの照合を行い、KsメモリB21にも時刻コード付きで鍵Ksを記憶しておけばよい。この場合も、時刻照合はC／N低下時のみ停止させればよい。

以上で本発明の基本的動作の説明はできたが、第3図と共に、第2図について説明を補足する。前述の通り第2図A，Bのヘツダーは6ビツトで、例えば第3図の如くb_0～b_5の値と、各パケツトの意味を対応させることができる。例えば1分間に使う鍵Ksが6個ではなく、10分間に使う鍵Ksを60個まとめて送ることとし、b_0～b_5の示す数値1～10を用いて複数の鍵Ksを含むパケツト（第2図A）を区別し、第4図、第5図の鍵Ksのメモリ容量を、時刻コードも含めて10倍にすれば、10分以下のC／N低下に対し同様の考え方で処理でき、C／N低下により鍵Ksを受信できなくなつても10分以内であれば引続きデスクランブルできる。なお、第2図Bの制御情報の中味は、システムに応じて決められる。

第6図は垂直期線期間を用いて鍵Ksを送るタイミング例を示す。先の説明では××分45秒を考える。B_1～B_nは、10秒毎に送る第2図Bの形式の信号の送出時点及び送出間隔を示し、B_1とB_2間は600フィールド離れている。一方A_1，A_7，……は本発明に示されるように鍵Ksをまとめて送る時点を示している。ここではB_1～B_nと同一フィールドの部分のみ、A_1，……A_7……を示している。拡大図に示す如く、15H目Ks50を送り、16H目にKs50～Ks40′を送れば、両方を同一フィールドで送ることができる。また10分単位で考えるときは、第7図の如く、1フィールドの11Hを用い、11H目に第2図B、12～21Hに第2図Aを10種類送ればよい。

前記実施例では、ラインパーミユテーションと呼ばれるスクランブル方式で説明したが、本発明

を他のスクランブル方式に適用できるのは勿論である。また、鍵を複数個（n個）送る場合には、間欠的又は連続的にこれを送ることができる。更に本発明の基本思想は、衛星放送以外の種々の有料放送システムに適用することが可能である。

［発明の効果］

以上の説明で明らかなように本発明によれば、個別に鍵を伝送するのに併せて、有料放送システムにおいて受信側で使用されるスクランブル解除のための解読鍵を時刻情報に関連させこれと共に所定時間分先に送つて記憶させ、通常は時々刻々変化する鍵を使用して、デスクランブルを行い、C／Nが低下したときには先に送られた鍵と時刻を照合し適切な鍵を使用することができるため、受信側でスクランブル解除を中断することがない。

4. 図面の簡単な説明

第1図は本発明の一実施例を示す回路構成図、第2図は2種類のデータパケツトを示す説明図、第3図はヘツダーの内容を表で示した説明図、第4図及び第5図は時刻と鍵の関係を表で示す説明図、

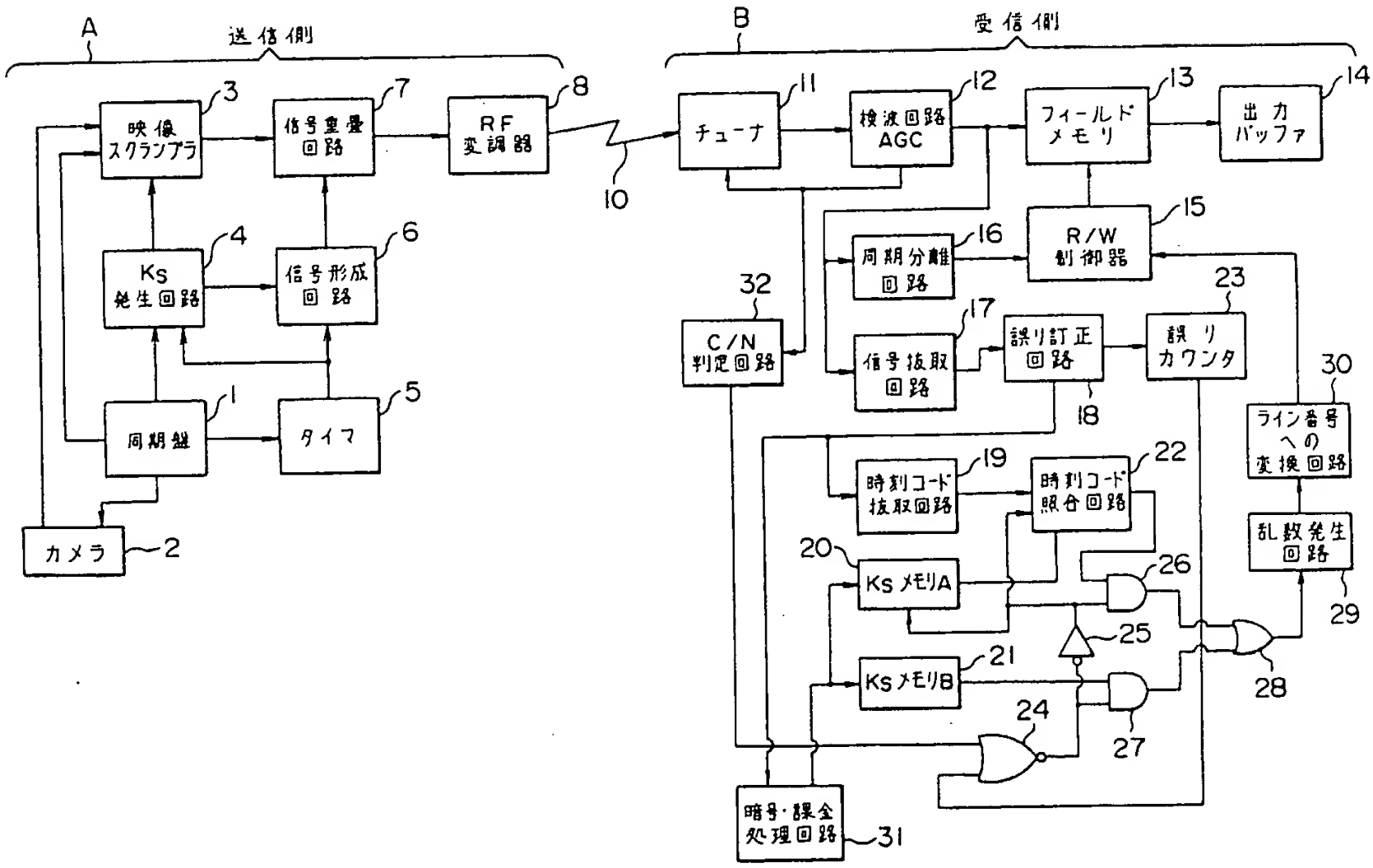
第6図及び第7図はデータパケツトの配置状態を示す説明図である。

［符号の説明］

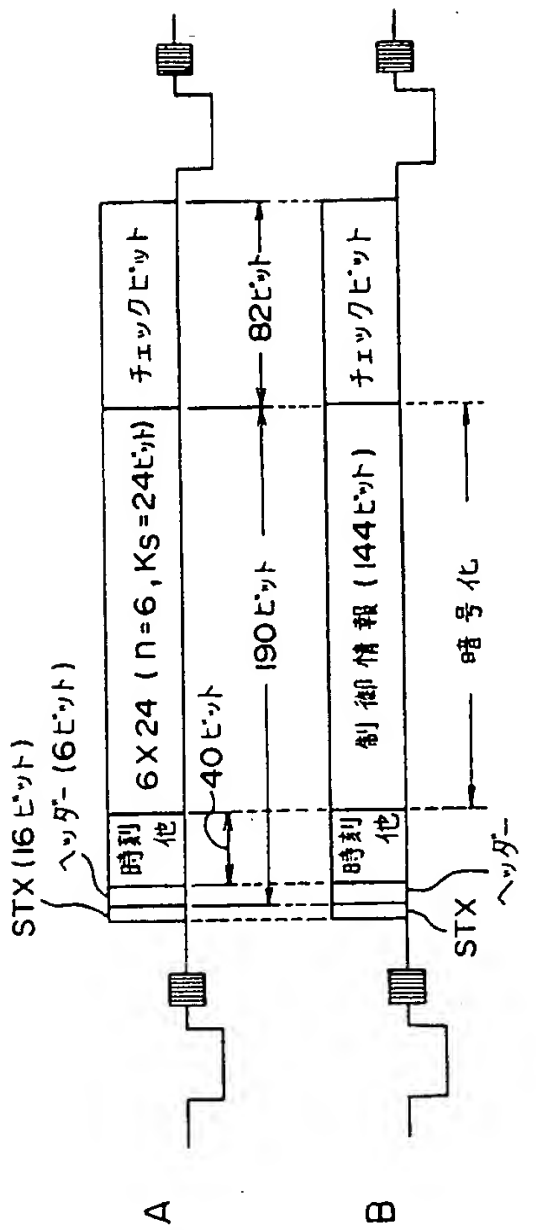
3…映像スクランブラ
4…Ks発生回路
7…信号重畳回路
13…フィールドメモリ
15…R／W制御器
19…時刻コード抜取回路
20…KsメモリA
21…KsメモリB
22…時刻コード照合回路
29…乱数発生回路
30…ライン番号への変換回路
31…暗号・課金処理回路
32…C／N判定回路

代理人　浅　村　　皓

第 1 図



第 2 図



第 3 図

ヘッダーの内容例

b_0	b_1	b_2	b_3	b_4	b_5	内容例
0	0	0	0	0	0	単独 Ks パケット
1	0	0	0	0	0	複数 Ks パケット No.1
0	1	0	0	0	0	複数 Ks パケット No.2
1	1	0	0	0	0	複数 Ks パケット No.3
0	0	1	0	0	0	複数 Ks パケット No.4
1	0	1	0	0	0	複数 Ks パケット No.5
0	1	1	0	0	0	複数 Ks パケット No.6
1	1	1	0	0	0	複数 Ks パケット No.7

LSB　MSB

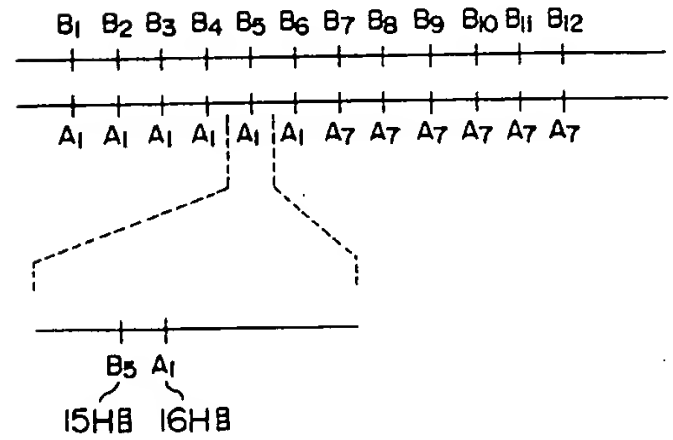
第 4 図

分		秒		Ks
X	X	1	0	K_{S10}
X	X	2	0	K_{S20}
X	X	3	0	K_{S30}
X	X	4	0	K_{S40}
X	X	5	0	K_{S50}
X	※	0	0	K_{S00}

第 5 図

分		秒		Ks
X	X	5	0	K_{S50}
X	※	0	0	K_{S00}
X	※	1	0	K_{S10}'
X	※	2	0	K_{S20}'
X	※	3	0	K_{S30}'
X	※	4	0	K_{S40}'

第 6 図



第 7 図